

# Securing Swarm Intellect Robots with a Police Office Model

I. A. Zikratov

Department of Secure Information  
Technologies  
ITMO University  
Saint-Petersburg, Russian Federation  
igzikratov@yandex.ru

I. S. Lebedev

Department of Secure Information  
Technologies  
ITMO University  
Saint-Petersburg, Russian Federation  
lebedev@cit.ifmo.ru

E. V. Kuzmich

Department of Secure Information  
Technologies  
ITMO University  
Saint-Petersburg, Russian Federation  
kekvlad@gmail.com

A. V. Gurtov

Helsinki Institute of Information Technology  
Finland  
Gurtov@hiit.fi

**Abstract** — This paper focuses on aspects of information security (IS) in group of mobile robotic systems with swarm intellect. It was justified requirements for IS mechanisms of swarm robotic systems. It was offered approaches to provide IS in swarm robotic systems, based on the implementation of the principles of centralized and decentralized security management of mobile agents. It was developed method of forming a self-organizing IS management system of robotic agents in swarm groups implementing POM (PoliceOfficeModel). It is presented a comparative analysis of the implementation of protected swarm systems depending on the logic of functioning police offices, integrated in swarm system.

**Index Terms**— IT security, robotic complex, swarm of a robot, ant algorithm, group robotics, PoliceOfficeModel, protected swarm, vulnerability, attack.

## I. INTRODUCTION

One of the areas of robotics which has received increasing attention is the group robotics. Application of the groups of mobile robots is characterized by the following conditions:

- unpredictable dynamics of the outdoor environment up to the conscious counter acting force;
- incomplete and contradictory knowledge of robots (agents) on the state of the outdoor environment and other participants;
- variety of options of attaining the goals, group structures, roles;
- complexity in providing reliable communication, groups distribution over a distance, etc.

It is obvious that these factors can be regarded as sources of threats that endanger the confidentiality and integrity of information circulating in the robotic system as well as the accessibility of elements in relevant information sphere. Perception of necessity to investigate issues of information security (IS) led to publication which contained a qualitative description of the main threats and the characteristics of their implementation for mobile robotic complexes (MRC) with swarm intellect [1, 2]. This paper demonstrates that swarm

MRC characterized by specific vulnerability, which, in turn, determines the necessity of the adaptation of scientific and methodological apparatus of IS to the conditions of operation of MRC. In particular, the unique swarm design features of robots make it difficult to use existing mechanisms of IS and gives attackers the opportunity to affect swarm algorithms (adaptive behaviour).

This article presents the research results of possible impacts of the opposing party on a swarm to increase task execution time by the group and/or reduce energy resources of robots, as well as provides a method of implementation of POM (PoliceOfficeModel – model based on police offices) to identify and prevent such attacks. The study was conducted on the basis of numerical modeling of a widely known classical ant shortest path algorithm [3].

The rest of the paper is organized as follows. In Section II, we give the background on the mobile robotic complexes utilizing the ant algorithm. In Section III, we introduce the police officer model for information security in robotic swarms. Section IV contains evaluation results of the model. Section V concludes the paper.

## II. MRC CONSTRUCTION WITH COLLECTIVE BEHAVIOR

Robotic complexes of collective behavior that implement the idea of a complex system consisting of a set of relatively simple devices are representatives of a relatively new and rapidly developing area of group robotics.

In this system agents possess several important features [4]:

- independence: agents, at least partially, are independent;
- limited representation: none of the agents know about the whole system, or the system is too complicated and its knowledge has no practical use for the agent;
- decentralization: there are no agents who manage the whole system.

Swarm groups are a variety of multi-agent robotic systems. The main difference in the implementation of a collective multi-agent system is in swarm management [5] and

availability of the communication channel via which robotic agents exchange data about their condition and current actions in the process of developing optimal solutions.

The ant algorithm is metaheuristic algorithm where a colony of artificial ants in joint cooperation finds a good solution of optimization of complex discrete problems. Using this algorithm when selecting the direction of movement, agents come not only from the selection of the shortest path, but also look at the experience of predecessors, leaving behind a special ferment (pheromone) at a path.

The numerical algorithm modeling the ant behavior was proposed. It is known that the selecting probability of the next agent at the time  $t$  can be calculated from the formula [3]:

$$\begin{cases} P_{ij,k}(t) = \frac{[\tau_{ij}(t)]^\alpha \cdot [\eta_{ij}]^\beta}{\sum_{n \in J_{i,k}} [\tau_{in}(t)]^\alpha \cdot [\eta_{in}]^\beta}, j \in J_{i,k}; \\ P_{ij,k}(t) = 0, j \notin J_{i,k} \end{cases} \quad (1)$$

where:  $P_{ij,k}(t)$  - probability of choosing the edge  $(i, j)$  by the agent  $k$  at the time  $t$ ;  $J_{i,k}$  - directions of robot's  $k$  movement;  $\eta$  - attraction, inversely proportional to the edge length ( $\eta = 1/D$ );  $\tau_{ij}(t)$  - pheromone level at time  $t$  on the edge  $(i, j)$ ;  $\alpha$  and  $\beta$  - two parameters that specify the weight for the pheromone trail and path visibility (its distance).

At  $\alpha = 0$  the robot's behavior will be "greedy", the closest point will be selected. If  $\beta = 0$ , then only pheromone effects will work out, and path selection will be based on the amount of pheromone on the route.

The ant algorithm is fully investigated, with possible variations, and the algorithm was used to solve various optimization problems [5,6,7].

### III. POLICE OFFICERS SECURITY MODEL

Analysis of the formula (1) suggests the possible ways of influencing the algorithm [2].

Numerical modeling of attacks on the swarm robotic complexes confirmed the conclusions of the authors of study [1] about the necessity to introduce the IS mechanisms, including the identification and authentication of the members of the swarm, and the use of "foreign" robot intruder detection. In addition, it was found that:

1. Physical integration into the swarm of subversive robots could have a destabilizing effect on the process of group in the transition process (in the process of finding the shortest path) as well as in the steady state when the shortest path is found. Consequently, measures to ensure IS should be carried out continuously at all stages of the task.

2. Effectiveness of the attack by subversive robots is determined by their flannerie long route, amount of integrated agents and concentration of used pheromone.

3. Attacks kind of the "wrong path" lead to the appearance of cyclical itineraries of swarm members ("back and forth", motion in a circle), which leads to unnecessary loss of time and energy by robots.

Common to all of the methods is the fact that the vulnerabilities inherent in ant algorithms allowed to carry out destructive effect on the swarm by information exposure

through sensors of agents without the attack on the physical and/or software component of the robot [8,9].

Obviously, in order to prevent the abovementioned attacks, swarm robotic complexes must be equipped with IS mechanisms that meet some specific requirements in comparison with the same protection mechanisms of multi-agent information systems [10,11,12,13,14]. There are two approaches to the implementation of such mechanisms to ensure IS: centralized and decentralized. In particular, the decentralized approach is based on the principle of mutual security, and represents a security system in which the agents are responsible for each other's security, tracking events occurring in the system and interacting with each other and outdoor environment. During interagent communications, system agents exchange information about their condition and actions through the communication channels as well as pass special messages that carry security information about the states of known agents and potential threats. Thus, all agents receive information about potential threats to their security. Informing their neighbors about possible dangers (e.g., when a "foreign" agent appears in the system), each of the agents is responsible for the safety of their environment and the system as a whole. The attractiveness of this model is in the absence of any single point of security, making it impossible to fracture model. However, the use of such systems for the swarm groups not equipped with communication channels may be subject to technical difficulties and rising costs of the system.

Therefore, to create a secure swarm robotic system is expedient to use a centralized approach to building security systems, where security features are assigned to specially created structures that in some models called Police Offices (PO). This article proposes a self-organizing mechanism for IS swarm systems based on PO model and aimed at preventing hidden attacks on swarm algorithms by subversive robots. Self-organization in this case means the automatic generation of police offices in the nodes of the graph routes (Figure 1), which are formed as a result of the ant algorithm functioning. Centralization provides a release of robotic agents who are members of the swarm of IS functions, and the imposition of these functions on special hardware and software complexes (integrated into the swarm model) implementing the PO functions and providing support interagent interaction and self-organization of the swarm.

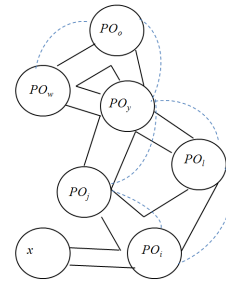


Fig. 1. Police offices and channels of interaction between them.

The structure of each PO is: 1) police agents on the number of nodes (vertices of the graph); 2) nodes register; 3) a database

of robotic agents; data encryption module (if necessary). Nearby PO are linked by communication channels.

The functioning logic for mobile agents information systems was proposed in the study [15]. Relating to the model of protected swarm logic of robotic agents interaction with police offices may be as follows:

#### Method 1.

Suppose that some robotic agent  $R_k$ , located at node  $i$ , selected according to the described ant algorithm the path of motion in the direction of node  $j$ . Agent  $R_k$  sends a request to the police agent  $AP_i$  of the office  $PO_i$  for resolution of the migration to the appropriate node. Police agent  $AP_i$  checks in its nodes registry the existence of the node  $j$ , and, if so, generates and outputs to the robotic agent  $R_k$  a unique certificate that contains: the agent identifier, energy level, information about the starting point and the selected route and time the certificate was issued. If necessary, data encryption of a robotic agent is carried out. After this procedure the agent authorizes police migration of  $R_k$ . Arriving at the node  $j$ , robotic agent  $R_k$  provides police agent  $AP_j$  of the node with a certificate. Police agent  $AP_j$  of the office  $PO_j$  based on information contained in the certificate checks in its nodes registry the existence of the node  $i$  and robotic agent  $R_k$  in police office certification center. If the information is confirmed, then  $AP_j$  refers to police agent  $AP_i$  of the office  $PO_i$  where the agent  $R_k$  migrated, which performs the functions of robotic agent certification center, asking to confirm the existence of the agent  $R_k$  and the fact that he was allowed to migrate to the node  $j$ . If the agent  $AP_i$  confirms the existence and migration of the agent  $R_k$  to node  $j$ , police agent  $AP_j$  settles motion time and energy parameters of the robotic agent from the node  $i$  to the node  $j$  to verify compliance of:

- real time of arrival and the power level of the agent, the estimated time of arrival and the energy level that can be calculated on the basis of their time of the departure from the node and the distance to it, and also the values of energy level at the time of departure of the robot from the node  $i$ ;
- the real path and the path that has been declared in the certificate correspondence.

In the absence of contradictory data the police agent  $AP_j$  enters robotic agent  $R_k$  into agents' database and gives it access to the resources of the node, necessary to solve the problems facing the swarm. For example, this may include information about the length of paths outside the site, which is required for the implementation of the algorithm to find the shortest path with parameter  $\alpha = 1$  in the formula (1). If necessary, at the  $PO_i$  site is making decryption of arrived agent.

If  $AP_j$  has not received an appropriate acknowledgment of the existence of the agent  $R_k$  in the system, or a mismatch on one of the test points (real changes in energy level, speed and direction of travel does not correspond to the declared values in the certificate), agent  $R_k$  is blocked, and access to resources for the node is prohibited. In this case police agent  $AP_j$  puts agent  $R_k$  into the "black list" and informs about the presence of

"foreign" agent in the system of all police offices it knows. Police agent  $AP_j$  carries similar actions if the robotic agent  $R_k$  as a further route selects the route by which it came to the node  $j$  because this is an indicative feature of the attack by means of method 1.

To prevent attacks by means of method 3 (attackers create "wrong path" routes) police agents have the blocking function of robotic agents for those routes that have the certificates issued by the same police office.

#### IV. PERFORMANCE EVALUATION OF A PROTECTED SWARM ALGORITHM

We will produce performance evaluation of a protected swarm algorithm by comparing task performance time of protected and unprotected swarm. For this we consider characteristics of system functioning at the stage of selecting the branch of the route, at the stage of movement along the branch and at the stage of arrival at a node of the route.

##### A. At the stage of selecting the route.

For unprotected system dead time  $T_1^U$  of the robotic agent will consist of time  $T_{RV}$  - the time required to calculate the shortest route according to ant algorithm. For a protected system the time  $T_{RAP}$  during negotiations with the police agent is added, working time of the police agent with the node registry  $T_{APU}$ , certification time for a robotic agent, and possible encryption of the agent data  $T_{KR}$ . Then, for a protected system dead time for an agent at the first stage will be:

$$T_1^P = T_{RV} + T_{RAP} + T_{APU} + T_{RV} + T_{KR} \quad (2)$$

##### B. At the stage of movement along the route.

At this stage, dead time of unprotected and protected swarm systems coincide, and equal to the time of movement of the robotic agent from the node  $i$  to the node  $j$ :

$$T_2^U = T_2^P = T_{ij} \quad (3)$$

##### C. At the stage of arrival to the destination node.

On arrival at the top of the graph the robotic agent proceeds to the selection of further route. Consequently, the dead time of the robotic agent  $T_3^U$  for unprotected algorithm in the node will consist of time  $T_{RV}$ .

For a protected system time costs will be determined by the following equation:

$$T_3^P = T_{RV} + T_{RAP} + T_{DKR} + T_{APU} + T_{UU} + T_{CalcR} + T_{BD} + T_{AR} \quad (4)$$

where:  $T_{RAP}$  - the negotiations time with the police agent;  $T_{DKR}$  - decrypting data time (if necessary),  $T_{APU}$  - conversion time of the agent to the nodes registry;  $T_{UU}$  - conversion time to the certification center (police office node of robotic agents' departure);  $T_{CalcR}$  - the time spent on calculation of parameters of the robotic agent according to the certificate,  $T_{BD}$  - conversion time to the database of the agents;  $T_{AR}$  - deciding time on the robotic agent according to the authentication results.

Obviously, the whole operation time depends on the complexity of the route, and accordingly, the necessary number of nodes PO layout as well as the amount of swarm. However,

the formulas (2) - (4) show that the greatest amount of time in the protected swarm algorithm is made to related procedures in matters of IB arrival node by the robotic agent:  $T_{UU}$ ,  $T_{CalcR}$ ,  $T_{BD}$  and  $T_{AR}$ . However, it should be noted that the time spent by robotic agent to overcome the distance between nodes  $T_{ij}$  is always greater than the value of  $T_{UU} + T_{CalcR} + T_{BD} + T_{AR}$ .

On this basis, we propose the following logic operation as part of a protected PO swarm.

#### D. Method 2.

##### 1) The first stage is selecting the route.

Suppose that some robotic agent  $R_k$  in node  $i$ , selects the path of motion in the direction of node  $j$ . Agent  $R_k$  sends a request to the police agent  $AP_i$  of the office  $PO_i$ , to allow the implementation of migration to the appropriate node. Police agent  $AP_i$  checks within its nodes registry and agents' database the existence of the node  $j$  and unique identifier of the robotic agent correspondingly. The police agent gives permission for migration for the agent  $R_k$ . The time required to perform these procedures will be:

$$T_1^2 = T_{RV} + T_{RAP} + T_{APU} + T_{BD}. \quad (5)$$

##### 2) The second stage is the movement of the agent along the route.

During the physical movement of the robotic agent from node to node at the police office node of the departure  $PO_i$  and arrival node  $PO_j$  robotic agent performs the following procedures:

Police agent  $AP_i$  certifies the departed robotic agent, which contains information on the energy level, information about the starting point, the selected route and arrival time of  $R_k$ . After that, the certificate encryption is occurring and sending it via the communication channels on the police office of the destination node of the robot  $R_k$ . To perform these actions it will need the time:

$$T_{RV} + T_{KR} + T_{UU} < T_{ij} \quad (6)$$

Police agent  $AP_j$  of the police office  $PO_j$  receives a certificate, decrypts it, and on the basis of information contained in the certificate checks in the nodes registry the existence of the node  $i$  in the system. If it is confirmed, the police agent  $AP_j$  calculates time and energy parameters of the robotic agent's motion from the node  $i$  to the node  $j$  to predict arrival time of the agent and energy level, which can be calculated on the basis of their time out of the departure node and the distance to it. The calculated results, as well as identifier and certificate of the agent  $R_k$ , police agent  $AP_j$  puts in the database of the office  $PO_j$ . Working time  $PO_j$  in data processing of the expected agent  $R_k$  is equal to:

$$T_{UU} + T_{DKR} + T_{APU} + T_{CalcR} < T_{ij}. \quad (7)$$

Thus, at this stage, dead time of the protected systems equals to the time during which the robotic agent moves from the node  $i$  to the node  $j$ :  $T_2^2 = T_{ij}$ .

##### 3) The third stage is the arrival at the top of the graph

At the third stage when robotic agent  $R_k$  arrived at node  $j$ , it produces its identifier to the police agent  $AP_j$  of the node. Police agent checks the identifier in the agents' database of its office  $PO_j$ . If it finds the certificate, then  $AP_j$  compares the real

time of arrival of the robot, its route and the power level of the agent with the data from the database of the office  $PO_j$  in relation to the agent  $R_k$ .

In the absence of contradictory data the police agent  $AP_j$  gives robotic agent  $R_k$  access to the resource information of the node, necessary to address the problems facing the swarm. If the data is not corresponding, police agent-police makes the lock-out procedures described previously in respect of the robot.

Dead time at the third stage is:

$$T_3^2 = T_{RV} + T_{RAP} + T_{BD} + T_{AR} \quad (8)$$

which is less by the amount of  $T_{DKR} + T_{APU} + T_{UU} + T_{CalcR}$ , than for implementing the method of providing a protected method of swarming system IS according the method 1 (Figure 2).

It should be noted, that when the swarm is performing tasks on rough terrain in the conditions of influence of destabilizing factors of natural and artificial origin, a significant role is acquired by robot group noise immunity. Let us consider the difference in the functioning of systems, organized by the described methods, under the influence of noise in communication channels between PO.

Considering, that in most cases the time of communication session  $T_{UU}$  is negligible in comparison with the time of moving of the agent from the  $i$ -th node to the  $j$ -th node ( $T_{UU} \ll T_{ij}$ ), the time  $T_{UU}$  can be neglected. Then for the method 1 the time of waiting of agent  $t_s^1$ , which arrived from the  $i$ -th node to the  $j$ -th node, will be:

$$t_s^1 = t_p, \quad (9)$$

$t_p$  – time of a malfunction or failure of communication channel under the influence of noise.

For the method 2

$$t_s^2 = \begin{cases} 0, & \text{if } T_{ij} < t_p \\ t_p - T_{ij}, & \text{if } T_{ij} \geq t_p \end{cases} \quad (10)$$

The formulas (09) - (10) show, that immunity of PO organization using the method 2 is potentially higher than using the method 1. The failure is only possible when the duration of noise exposure exceeds the time of moving agent from node to node. In addition, when the number of agents arriving in node or their movement speed increases, the effect of DDoS attacks (Distributed Denial of Service) may appear, when the number of requests of the robot to PO increases sharply. In this case organization using the method 1 requires increasing productivity of data transfer.

The experiment that simulates the movement of the agent from one node to another under the impact of communication channel by the noise with random duration and with random turn-on time of noise generator was conducted. The initial data: time of agent moving – 12 sec, duration of noise – from 3 to 56 sec.

The results of simulation are shown in Figure 3.

The Figure 3 shows, that by the implementation of the method 2, the effect of noise does not influence on the operation of secure algorithm with the condition  $T_{ij} < t_p$ , that confirms the formula (10).



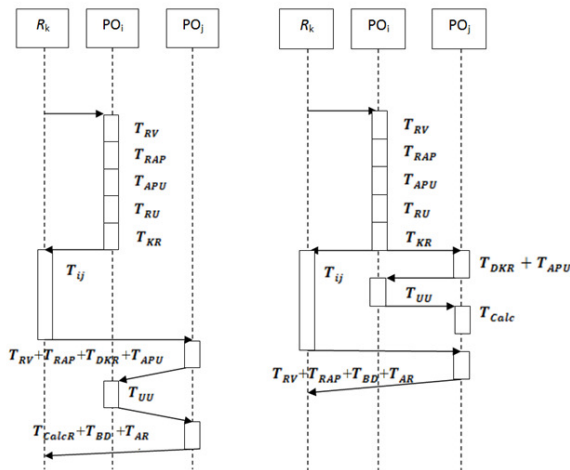


Fig. 2. The diagram of interaction of PO main components. Organization of interaction in method 1 and method 2

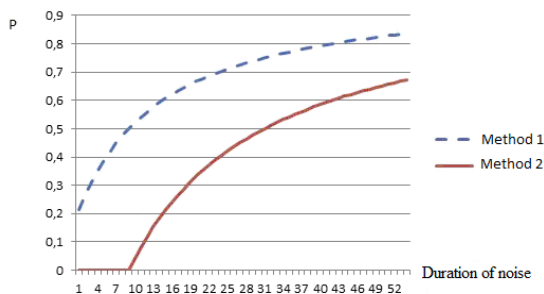


Fig. 3. Dependence of the probability of PO failure of servicing the agent on the duration of noise in the communication channel between police stations.

## V. CONCLUSIONS

This paper analyzes hidden attacks on robotic systems with swarm intellect. We proposed solving problems of information security of agents in robotic multi-agent systems. During the studies we obtained the following results:

1) We formulated requirements for IS mechanisms of swarm robotic systems. The advantages and disadvantages of approaches to information security in swarm robotic systems, based on the implementation of the principles of centralized and decentralized security management of mobile agents were considered.

2) We developed a method of forming a self-organizing IS management system of robotic agents of swarm groups implementing POM, which applies to IS in multi-agent systems. The method consists of integration to the group of robots software and hardware components that perform functions of detection and prevention attacks on hidden swarm algorithms.

3) We conducted the analysis of the logic operation of information security management system by robotic agents in swarm groups. We performed a comparative analysis of the implementation of protected swarm systems depending on the

logic of functioning police offices, integrated in a swarm system.

4) A numerical experiment of secure algorithm, including simulating work in noising environment was conducted.

## REFERENCES

- [1] Higgins F., Tomlinson A., Martin K.M. Threats to the Swarm: Security Considerations for Swarm Robotics // International Journal on Advances in Security, Vol. 2, No. 2&3, 2009, pp. 288 – 297.
- [2] Zikratov I.A., Zikratova T.V, Kozlova E.V. Vulnerability analysis of robotic systems with swarms intelligence // Scientific and Technical Journal of Information Technologies, Mechanics and Optics -2013 . - № 5 (87). - pp. 149-154.
- [3] Dorigo M., V. Maniezzo & A. Colorni, 1996. "Ant System: Optimization by a Colony of Cooperating Agents", IEEE Transactions on Systems, Man, and Cybernetics–Part B, 26 (1): 29–41.
- [4] Michael Wooldridge, An Introduction to MultiAgent Systems, John Wiley & Sons Ltd, 2002, paperback, 366 pages, ISBN 0-471-49691-X.
- [5] Kalyaev I.A., Gayduk A.R., Kapustyan S.G. Modeli i algoritmy kollektivnogo upravleniya v gruppakh robotov.– M.: Fizmatlit, 2009. - 280 c.
- [6] Ermolaev S.U. Muravinye algoritmy optimizatsii. // Infokommunikatsionnye tekhnologii. Tom 6., № 1, 2008. P. 23 – 29.
- [7] Jean-Baptiste Waldner. Nanocomputers and swarm intelligence. London, ISTE, 2007, p. 242-248
- [8] Lefevr V.A. Konfliktuyuschiye. – M.: Sovetskoye radio, 1973.
- [9] Wheeler, W. M. Ants: their structure, development and behavior. — New York, Columbia University Press, 1910. — P. 265.
- [10] Neeran K.M., Tripathi A.R. Security in the Ajanta MobileAgent system. Technical Report. Department of Computer Science, University of Minnesota, May 1999.
- [11] Sander T., TschudinCh.F. Protecting MobileAgents against malicious hosts. In Giovanni Vigna (ed.) MobileAgents and Security, LNCS, Springer, p.44-60, 1998.
- [12] Xudong G., YilingYa., Yinyuan Y. POM-a mobile agent security model against malicious hosts. Proceedings of High Performance Computing in the Asia-Pacific Region , v.2, p.1165-1166, 2000.
- [13] Page J., Zaslavsky A., Indrawan M. A Buddy model of security for mobile agent communities operating in pervasive scenarios. Proceeding of the 2 nd ACM Intl. Workshop on Australian Information Security & Data Mining, v.54, 2004.
- [14] Page, A. Zaslavsky, and M. Indrawan. Countering security vulnerabilities using a shared security buddy model schema in mobile agent communities. Proc. of the First International Workshop on Safety and Security in Multi-Agent Systems (SASEMAS 2004), pages 85–101, 2004.
- [15] Masloboev A.V., Putilov V.A. Razrabotka i realizatsiya mekhanizmov upravleniya informatsionnoy bezopasnostiyu mobilnikh agentov v raspredelennykh multiagentnykh informatsionnykh sistemakh // Vestnik MGTU. – 2010. – Tom 13, №4/2. – s. 1015-1032.